AMENDMENTS TO THE CLAIMS

Claims 1-9, 11-24, 26-42 and 44-56 are pending. Please amend claims 1, 19, and 39, as set forth below to correct for grammatical issues, without acquiescence in the Office Action's reasons for rejection or prejudice to pursue in a related application. No new matter has been added. A complete listing of the pending claims is provided below.

1. (Currently Amended) A computer-implemented method for managing user access information for access to one or more database network nodes by a user, the method comprising:

storing database user authorization in a central directory that is associated with one or more network nodes, the database user authorization comprising a user role associated with a collection of locally defined roles and associated users, wherein the user role in the central directory assigns user privileges to the user as defined by the locally defined roles contained within the user role, wherein the database user authorization is stored as one or more data objects in the central directory;

storing database user authentication information;

receiving the user role at a local database network node from the central directory;

locally defining, by using a processor, a locally defined role for assigning the user privileges specific to a local database network node for a local scope of access at the local database network node, wherein the locally defined role is locally defined by processing at the local database network node the user role that is received from the central directory, and the user privileges granted by the locally defined role [[is]] are given to the user based at least in part upon the user's association with the user role ~~as provided by the user role~~ such that the locally defined role has a different scope of access than another locally defined role defined by processing the same user role at another local database network node;

receiving an access request from the user for the local database network node;

authenticating the user using a shared schema based at least in part upon the database user authentication information, wherein the shared schema comprises a schema that is accessible by a plurality of users and the plurality of users are mapped to the shared schema on the local database network node such that the plurality of users do not need their own accounts on the local database network node;

granting the user privileges on the local database network node based at least in part upon the shared schema and the locally defined role; and

storing the user privileges in a volatile or non-volatile computer-usable medium or displaying the user privileges on a display device.

2. (Original) The method of claim 1 in which the central directory comprises a LDAP-compatible directory.

3. (Original) The method of claim 1 in which the database user authentication information is stored at the central directory.

4. (Original) The method of claim 1 in which the database user authorization is stored in a schema having a hierarchy of schema objects.

5. (Original) The method of claim 4 in which the hierarchy of schema objects comprises an enterprise role, wherein the enterprise role is associated with one or more users and one or more locally defined roles.

6. (Previously Presented) The method of claim 5 in which the one or more privileges are assigned to the one or more users.

7. (Original) The method of claim 4 in which the hierarchy of schema objects comprises a enterprise domain, wherein the enterprise domain comprises one or more enterprise roles.

8. (Original) The method of claim 7 in which each of the one or more enterprise roles is associated with one or more users and one or more locally defined roles.

9. (Original) The method of claim 7 in which the enterprise domain is associated with one or more network nodes.

10. (Canceled)

11. (Previously Presented) The method of claim 1 in which the one or more data objects are stored in a security subtree in the central directory.

12. (Original) The method of claim 1 in which administrative access is controlled to one or more data objects in the central directory.

13. (Original) The method of claim 12 in which access control is implemented using an access control point associated with the one or more data objects in the central directory.

14. (Original) The method of claim 13 in which the access control point is associated with access policies for a subtree of the one or more database objects in the central directory.

15. (Original) The method of claim 13 in which the access control point is associated with access policies for a single entry for the one or more database objects in the central directory.

16. (Original) The method of claim 13 in which the access control point is associated with individually named users.

17. (Original) The method of claim 13 in which the access control point is associated with a group of users.

18. (Original) The method of claim 17 in which members of the group are associated with a set of access privileges associated with the access control point.

19. (Currently Amended) A computer system including a processor for managing user access information for access to one or more database network nodes by an enterprise user, comprising:

a LDAP directory;

one or more local database network nodes for which user access is sought, wherein the one or more local database network nodes are associated with the LDAP directory;

a volatile or non-volatile computer-usable medium for storing user access information data objects in the LDAP directory, the user access information data objects comprising authentication and authorization information, wherein the authorization information comprises an enterprise role associated with a collection of locally defined roles and associated users, wherein the enterprise role in the LDAP directory assigns user privileges to the enterprise user as defined by the locally defined roles contained within the enterprise role; and

the processor for locally defining a locally defined role for assigning the user privileges specific to a local database network node for a local scope of access at the local database network node, wherein the locally defined role is locally defined by processing at the local database network node the enterprise role that is received from the LDAP directory, and the user privileges granted by the locally defined role are given to the enterprise user based at least in part upon the enterprise user's association with the enterprise role ~~as provided by the enterprise role~~ such that the locally defined role has a different scope of access than another locally defined role defined by processing the same enterprise role at another local database network node.

20. (Original) The system of claim 19 in which the user access information data objects comprise a domain object that is associated with the one or more database network nodes.

21. (Previously Presented) The system of claim 20 in which the domain object is associated with the enterprise role.

22. (Original) The system of claim 21 in which the enterprise role is associated with a local database role.

23. (Original) The system of claim 22 in which the scope of the local database role is locally defined at a local database network node.

24. (Previously Presented) The system of claim 21 in which the enterprise role is associated with another user.

25. (Canceled).

26. (Original) The system of claim 19 in which the user access information data objects comprise an access control point attribute.

27. (Original) The system of claim 26 in which the access control point attribute is established only if access control policies are established for a corresponding object.

28. (Original) The system of claim 26 in which the access control point attribute is associated with access policies for a subtree in the user access information data objects stored in the LDAP directory.

29. (Original) The system of claim 26 in which the access control point attribute is associated with access policies for a single entry in the user access information data objects stored in the LDAP directory.

30. (Original) The system of claim 26 in which the access control point attribute is associated with individually named users.

31. (Original) The system of claim 26 in which the access control point attribute is associated with a group of users.

32. (Previously Presented) The system of claim 31 in which members of the group are associated with a set of access privileges associated with the access control.

33. (Original) The system of claim 19 in which the user access information data objects comprise a mapping object that maps an database user to a database schema.

34. (Original) The system of claim 33 in which the mapping object affects a single user.

35. (Original) The system of claim 34 in which the mapping object is associated with a full distinguished name.

36. (Original) The system of claim 33 in which the mapping object is associated with a plurality of users.

37. (Original) The system of claim 36 in which the mapping object is associated with a partial distinguished name.

38. (Original) The system of claim 21 in which the enterprise role is associated with local database roles from a plurality of database nodes.

39. (Currently Amended) A computer program product that includes a volatile or non-volatile non-transitory computer-usable medium usable by a processor, the medium having stored thereon a sequence of instructions which, when executed by said processor, causes said processor to execute a process for managing user access information for access to one or more database network nodes by a user, the process comprising:

storing database user authorization in a central directory that is associated with one or more network nodes, the database user authorization comprising a user role associated with a collection of locally defined roles and associated users, wherein the user role in the central directory assigns user privileges to the user as defined by the locally defined roles contained within the user role, wherein the database user authorization is stored as one or more data objects in the central directory;

storing database user authentication information;

receiving the user role at a local database network node from the central directory;

locally defining a locally defined role for assigning the user privileges specific to a local database network node for a local scope of access at the local database network node, wherein the locally defined role is locally defined by processing at the local database network node the user role

that is received from the central directory, and the user privileges granted by the locally defined role [[is]] are given to the user based at least in part upon the user's association with the user role ~~as provided by the user role~~ such that the locally defined role has a different scope of access than another locally defined role defined by processing the same user role at another local database network node;

receiving an access request from the user for the local database network node;

authenticating the user using a shared schema based at least in part upon the database user authentication information, wherein the shared schema comprises a schema that is accessible by a plurality of users and the plurality of users are mapped to the shared schema on the local database network node such that the plurality of users do not need their own accounts on the local database network node;

granting the user privileges on the local database network node based at least in part upon the shared schema and the locally defined role; and

storing the user privileges or displaying the user privileges on a display device.

40. (Previously Presented) The computer program product of claim 39 in which the central directory comprises a LDAP-compatible directory.

41. (Previously Presented) The computer program product of claim 39 in which the database user authentication information is stored at the central directory.

42. (Previously Presented) The computer program product of claim 39 in which the database user authorization is stored in a schema having a hierarchy of schema objects.

43. (Canceled)

44. (Previously Presented) The computer program product of claim 39 in which the one or more objects are stored in a security subtree in the central directory.

45. (Previously Presented) The computer program product of claim 39 in which administrative access is controlled to one or more data objects in the central directory.

46. (Previously Presented) The computer program product of claim 45 in which access control is implemented using an access control point associated with the one or more data objects in the central directory.

47. (Previously Presented) The computer program product of claim 46 in which the access control point is associated with access policies for a subtree of the one or more database objects in the central directory.

48. (Previously Presented) The computer program product of claim 46 in which the access control point is associated with access policies for a single entry for the one or more database objects in the central directory.

49. (Previously Presented) The computer program product of claim 46 in which the access control point is associated with individually named users.

50. (Previously Presented) The computer program product of claim 46 in which the access control point is associated with a group of users.

51. (Previously Presented) The computer program product of claim 50 in which members of the group are associated with a set of access privileges associated with the access control point.

52. (Previously Presented) The method of claim 1, wherein one of the one or more data objects comprises a distinguished name, wherein the distinguished name comprises a common name having a value for identifying a database.

53. (Previously Presented) The method of claim 1, wherein one of the one or more data objects comprises a distinguished name, wherein the distinguished name comprises a common name having a value for representing an administrative context, a root context, or a user-fined context.

54. (Previously Presented) The method of claim 1, wherein the one or more privileges are locally defined at the one of the network nodes.

55. (Previously Presented) The method of claim 54, wherein the database user authorization is stored in the central directory such that central management of the user role may be performed.

56. (Previously Presented) The method of claim 54, wherein the one or more privileges are not centrally defined at the central directory.